OAuth integration

Carina supports OAuth v2 for integration with external applications. OAuth is an authentication protocol that allows users to grant limited access to their account without sharing their password. With Carina OAuth, you can authenticate users, download their cluster credentials, and create clusters on their behalf.

* [OAuth dance](https://staging.developer.rackspace.com/getcarina.com/build-85b6c1f5d0/docs/reference/oauth-integration/%22%20%5Cl%20%22oauth-dance)
* [Register your application](https://staging.developer.rackspace.com/getcarina.com/build-85b6c1f5d0/docs/reference/oauth-integration/#register-your-application)
* [Configure your application](https://staging.developer.rackspace.com/getcarina.com/build-85b6c1f5d0/docs/reference/oauth-integration/#configure-your-application)
* [Interact with Carina](https://staging.developer.rackspace.com/getcarina.com/build-85b6c1f5d0/docs/reference/oauth-integration/#interact-with-carina)

OAuth dance

The flow that a user experiences when authorizing an application is sometimes called the "OAuth dance" because of the back-and-forth communication between the external application and OAuth provider. The following process describes that dance with Carina.

1. The external application requests permission to access the user's Carina account. Usually this request happens when a user clicks a login or authorize button on the application’s website.



1. The user is redirected to the Carina OAuth website. If the user is not logged in, the user is prompted for Rackspace credentials. These credentials are used to authenticate the user against Carina and are not shared with the external application.



1. The user is presented with an authorization form that lists the permissions requested by the application.



1. After the application is authorized, the user is redirected back to the application.

Authorized applications can act on behalf of the user until that authorization is revoked. You can view a list of authorized applications on the Carina OAuth website and revoke an application's access.



Register your application

Before your application can integrate with Carina, you must first register the application.

1. Log in to the [Carina OAuth](https://oauth.getcarina.com/) website.
2. On the Developer Applications page, click New Application.



1. Complete the registration form. The Redirect URI specifies the URL to which users are directed after they authorize your application. It must be a secure web page, starting with https.



On the confirmation page, the application ID and secret are displayed. Do not share the secret publicly, and do not check it in to source control.



Configure your application

Select an [OAuth2 library](http://oauth.net/2/) for the programming language used by your application. Depending on the library, some or all of the following configuration is handled by the library. The following guidelines are generic; see the documentation for your particular library for additional details.

1. In your application, configure the library to use the application ID, secret, and callback URL assigned to your registered application in the Carina OAuth Control Panel.
2. Add a link to your application that requests access to the user's Carina account. Replace <applicationId> and <redirectURI> with the values from your application registration.

https://oauth.getcarina.com/oauth/authorize?client\_id=<applicationId>&redirect\_uri=<redirectURI>&response\_type=code

The scope query string parameter is optional and should be a space separated list of the requested scopes.

&scope=identity+cluster\_credentials+create\_cluster

1. Add a web page to your application that handles requests to your Redirect URI.

After the user authorizes your application, the user is redirected to this page with the authorization code included in the query string.

https://example.com/carina-oauth-callback?code=abc123

The callback web page should use the authorization code to request a token, and then store the returned tokens. The access\_token value has an expiration date, after which the refresh\_token value can be used to request a new token.

Example request

POST https://oauth.getcarina.com/oauth/token

{

 "client\_id": "<applicationId>",

 "client\_secret": "<secret>",

 "redirect\_uri": "<redirectURI>",

 "code": "<authorizationCode>",

 "grant\_type": "authorization\_code"

}

Example response

{

 "access\_token": "09ba487fc3df...",

 "token\_type": "bearer",

 "expires\_in": 7200,

 "refresh\_token": "8c488ab5f75d61..."

}

Interact with Carina

The following OAuth scopes are available, granting your application varying levels of access to a user's account.

* [Identity](https://staging.developer.rackspace.com/getcarina.com/build-85b6c1f5d0/docs/reference/oauth-integration/#identity-scope)
* [Cluster credentials](https://staging.developer.rackspace.com/getcarina.com/build-85b6c1f5d0/docs/reference/oauth-integration/%22%20%5Cl%20%22cluster-credentials-scope)
* [Create cluster](https://staging.developer.rackspace.com/getcarina.com/build-85b6c1f5d0/docs/reference/oauth-integration/%22%20%5Cl%20%22create-cluster-scope)

All requests must include an authorization header, Authorization: bearer <access\_token>, replacing<access\_token> with the OAuth token returned from the /oauth/token endpoint.

Identity scope

The identity scope enables an application to read a user's profile. Because the amount of information in a user’s profile is limited, this scope is mainly useful for delegating your application's authentication to Carina.

Example request

GET https://oauth.getcarina.com/me

Example response

{

 "id": 1,

 "username": "carolynvs",

 "email": "carolyn.vanslyck@rackspace.com",

 "full\_name": "carolynvs"

}

Cluster credentials scope

The cluster\_credentials scope enables an application to download the credentials zip file for a user’s Carina cluster. Replace <clusterName> with name of the cluster.

Example request

GET https://oauth.getcarina.com/clusters/<clusterName>

Example responses

The body of the response is the user's cluster credentials zip file, provided as an application/zip encoded binary attachment.

If the cluster is not yet active, a 404 NOT FOUND response is returned. After a new cluster is created, it can take 2-3 minutes for the cluster to become active. Poll the cluster credentials endpoint at a reasonable interval, such as every 30 seconds, until the cluster is active.

{

 "message": "The cluster is not yet active. Retry this request later."

}

Create cluster scope

The create\_cluster scope enables an application to create a cluster on the user’s Carina account. If the cluster already exists, the request succeeds and the cluster information is returned. Replace <clusterName> with the name of the cluster to create.

Example request

PUT https://oauth.getcarina.com/clusters/<clusterName>

Example response

{

 "cluster\_name": "<clusterName>",

 "status": "building",

 "autoscale": false,

 "flavor": "container1-4G",

 "nodes": 1

}

Resources

* [OAuth2 libraries](http://oauth.net/2/)
* [OAuth2 authorization code grant workflow](https://tools.ietf.org/html/rfc6749#section-4.1)